Session 305

Extending Security in Mac OS X

Craig Keithley
Security & Cryptography Technology Manager
Worldwide Developer Relations

Session 305

Extending Security in Mac OS X

John Hurley, Ph.D.
Manager, Data Security

Introduction

- Mac OS X gives us a great platform to implement security features
- We have some great features to help developers implement their security solutions
- Configurable

What You'll Learn

- Apple's architecture for Data Security
- The foundation for our security architecture: CDSA
- Keychain API overview
- Authorization API overview
- Core OS security

Mac OS X Opportunities

- Protected memory
  - Keys in separate address space
- Multitasking
- BSD infrastructure
- Fresh start
- Announcement…

Open Source

- We are open sourcing many components of the Apple Data Security Architecture!
- All subprojects of Security.framework
- Allows for peer review
- Easier export compliance
- We value your contributions

Open Source Components

- Sub-projects of Security.framework:
  - Authorization, SecureTransport, Keychain and SecurityServer
- Default plugin modules and utility frameworks
  - AppleDL (DL), AppleCSP (CSP), AppleCSPDL (CSP/DL), AppleX509CL (CL), AppleX509TP (TP), SecuritySNACCRuntime, SecurityASN1, and cdsa_utilities

Keychain

- Every user on Mac OS X has a Keychain
- Unlocked with login password
- If you need to save a password somewhere, use the Keychain!
- Usually totally transparent to users
- Available through Carbon

Authorization API

- Authorization vs. Authentication
  - Authorization is yes/no for operation
  - Do I have the ability to do something?
- Authentication
  - May establish identity
  - Who you are, what you know, what you have
  - Optionally produces some sideband info
  - May succeed trivially

Authorization API (Cont.)

- Operation: log in at console
  - Authentication steps could include:
    - Type user name and password
    - Insert smartcard
    - Fingerprint
    - Voice recognition
- Examples of operations
  - Unlock screensaver
  - Play a CD
  - Format a disk

CDSA

- Common Data Security Architecture
- OpenGroup standard
- Uses plugin modules
  - Data Library (DL)
  - Cryptographic Service Provider (CSP)
  - Certificate Library (CL)
  - Trust Policy (TP)

Apple Security Architecture

Security Applications

- Others
- Keychain Access
- URL Access

Layered Services

- Security Core
- Security HI
- SecureTransport

CSSM Security API

Add-in Modules

- Security Server
- Access Control
- Data Library
- Apple File CSP/DL
- Trust Policy
- Cryptographic Service Provider
- Certificate Library

Data Library Modules (DLs)

- Store information used by other CDSA modules
- Apple File CSP/DL
  - A combination CSP/DL (encrypts and stores)
  - Keychains are flat files maintained by this CSP/DL
- Other Examples
  - LDAP DL

Certificate Library Modules (CLs)

- Interpret public key certificates
- Examples
  - Apple CL interprets X.509 v3 certificates
  - PGP CL
  - Attribute CL

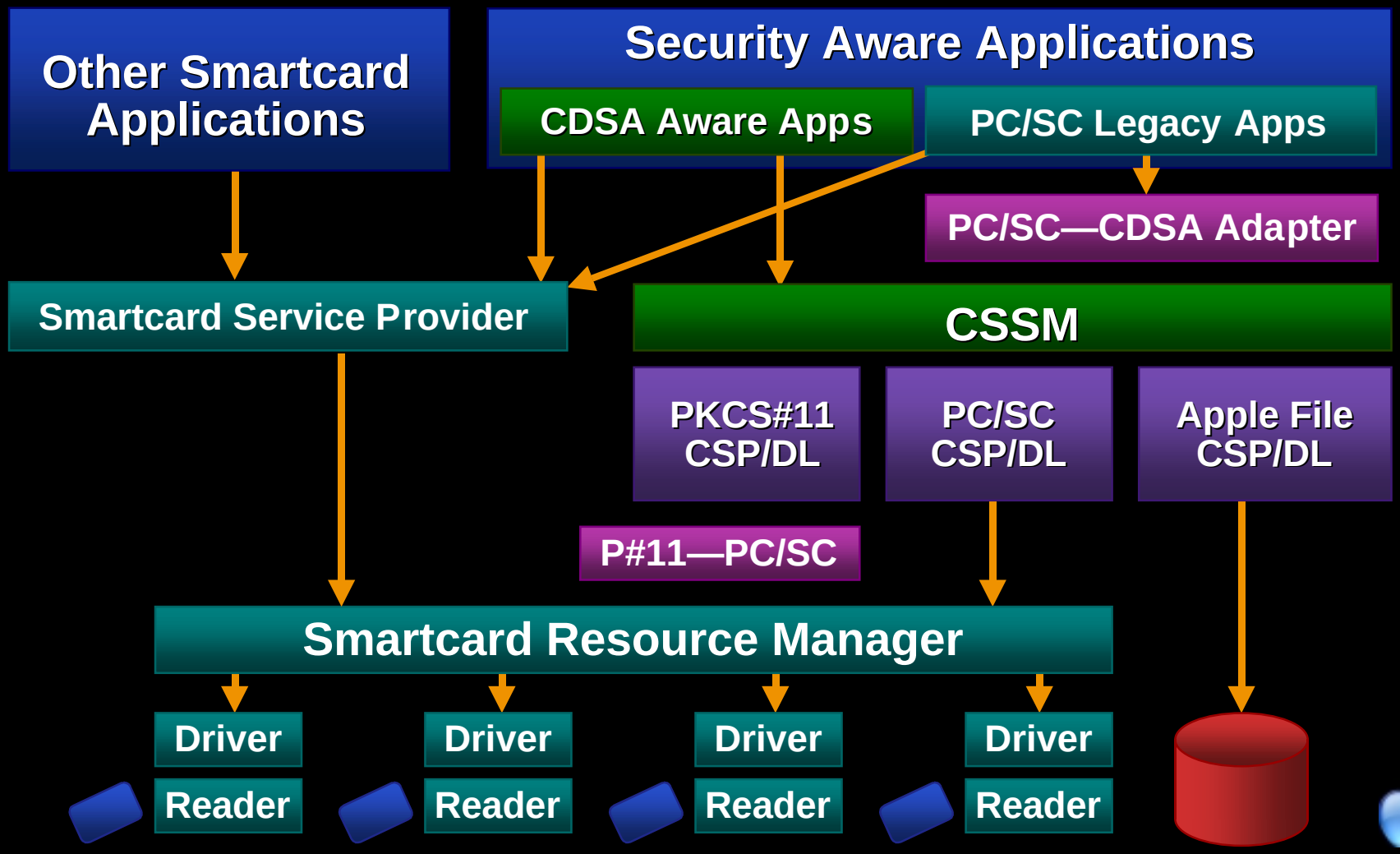
Trust Policy Modules (TPs)

- Encapsulate how certificates should be evaluated for trust decisions
- Examples
  - A corporate TP could reject any certificate chain that did not contain the corporate certificate in the chain
  - Could implement web-of-trust instead of chain of trust

Smartcards with PC/SC

- Allow easy access to CDSA APIs
- Current applications using PC/SC
- Apple will try to minimize coding impact for:
  - Hardware developers writing drivers for readers
  - Applications written to PC/SC on other platforms
  - Card developers writing CSPs for cryptography

Apple PC/SC Architecture



Core Level Security

- Mac OS X ships with most services off
- Root password disabled by default but can be re-enabled
- File permissions are designed to work with Mac OS 9
- Use the tricks you know from UNIX

Resources

Security
Specifications and SDKs
http://developer.apple.com/macos/security.html

CDSA 2.0
Specifications
http://www.opengroup.org

PC/SC
Specifications
http://www.pcscworkgroup.com

Related Sessions

306 Security: Authorization APIs Interfaces for HTTP & FTP	Hall J2 **Wed., 10:30am**
307 Security: Keychain High level access to the keychain	Hall J2 **Wed., 2:00pm**
309 Security: Kerberos Learn about Kerberos	Hall A2 **Thurs., 2:00pm**
FF113 Feedback Forum: Security Talk to us	Hall C **Fri., 10:30am**

Who to Contact

Worldwide Developer Relations
Craig Keithley
Security & Cryptography Technology Manager
keithley@apple.com

Q&A

Craig Keithley
Security & Cryptography Technology Manager
keithley@apple.com

http://developer.apple.com/events/urls.html

WWDC

Worldwide Developers Conference 2001